Russian Technological Journal.
2025;13(6):25–46

ISSN 2782-3210 (Print)
ISSN 2500-316X (Online)

УДК 004.387
https://doi.org/10.32362/2500-316X-2025-13-6-25-46
EDN XEUFSE

НАУЧНАЯ СТАТЬЯ

Подход к выявлению оптимального набора кубит квантовых вычислительных устройств на примере модели генерации случайных двоичных последовательностей

А.В. Корольков,
А.А. Крючков @

МИРЭА – Российский технологический университет, Москва, 119454 Россия
@ *Автор для переписки, e-mail: kryuchkov_a@mirea.ru*

• **Поступила:** 23.12.2024 • **Доработана:** 15.05.2025 • **Принята к опубликованию:** 06.10.2025

Резюме

Цели. Отсутствие квантовых компьютеров, устойчивых к ошибкам, а также невозможность обеспечить беспрепятственный и полнофункциональный физический доступ к облачным квантовым системам поднимает актуальный вопрос о необходимости разработки методов оценки и верификации облачных квантовых компьютеров. Авторам видится перспективным использование подхода к анализу возможностей квантового процессора в контексте его применимости для решения некоторых задач, возникающих при оценке систем защиты информации. Одним из примеров теста квантового вычислительного устройства (КВУ) на предмет выявления уровня производительности и качества вычислений может послужить модель генерации случайной двоичной последовательности, анализ которой предоставляет информацию о корректности и надежности исследуемого квантового регистра. Цель работы заключается в разработке программного комплекса, с помощью которого представляется возможным моделирование работы КВУ в режиме квантового генератора случайных чисел.

Методы. Программная реализация по взаимодействию с облачными квантовыми компьютерами выполнена с использованием библиотеки Qiskit. Интерфейс программного комплекса реализован средствами Qt5, кроссплатформенного набора инструментов и виджетов для создания графических приложений. Анализ генерируемой двоичной последовательности выполнен статистическими тестами NIST STS[1].

Результаты. Разработан программный комплекс, предоставляющий пользователю в графическом режиме возможность выполнения опционального исследования некоторых облачных квантовых компьютеров на предмет выявления оптимального и наиболее устойчивого к ошибкам набора кубит. Приведены результаты экспериментов на трех облачных КВУ.

[1] The National Institute of Standards and Technology, Statistical Test Suite – Национальный институт стандартов и технологий США, набор статистических тестов.

Выводы. В условиях накладываемых ограничений на вычислительные мощности и время использования облачных КВУ предложенный подход отличается минимальными требованиями к производительности устройства, предоставляет наглядные и однозначно-интерпретируемые сведения об исследуемых технических характеристиках квантового компьютера, является воспроизводимым, легко масштабируемым и универсальным.

Ключевые слова: квантовый компьютер, квантовое вычислительное устройство, генератор случайных чисел, оценка производительности

Для цитирования: Корольков А.В., Крючков А.А. Подход к выявлению оптимального набора кубит квантовых вычислительных устройств на примере модели генерации случайных двоичных последовательностей. *Russian Technological Journal*. 2025;13(6):25–46. https://doi.org/10.32362/2500-316X-2025-13-6-25-46, https://www.elibrary.ru/XEUFSE

Прозрачность финансовой деятельности: Авторы не имеют финансовой заинтересованности в представленных материалах или методах.

Авторы заявляют об отсутствии конфликта интересов.

RESEARCH ARTICLE

Approach for identifying the optimal set of qubits of quantum computing devices based on a model for generating binary random sequences

Andrey V. Korolkov,
Andrey A. Kryuchkov @

MIREA – Russian Technological University, Moscow, 119454 Russia
@ *Corresponding author, e-mail: kryuchkov_a@mirea.ru*

• **Submitted:** 23.12.2024 • **Revised:** 15.05.2025 • **Accepted:** 06.10.2025

Abstract

Objectives. The absence of error-resistant quantum computers, coupled with the challenges associated with providing unrestricted and fully operational physical access to cloud quantum computing systems, prompts a critical examination of the necessity to develop universal and independent methods for evaluating and verifying cloud quantum computers. A promising approach involves evaluating the capabilities of a quantum computer in relation to its effectiveness in addressing specific challenges encountered in the assessment of information security systems. A potential test for ascertaining the performance and computational quality of a quantum computing device (QCD) is based on a model designed to generate a random binary sequence. By analyzing this sequence, insights can be obtained into the accuracy and reliability of the quantum register under study. The paper presents a software program developed for simulating the operation of a quantum random number generator.

Methods. The software implementation for interacting with cloud quantum computers was performed using the Qiskit open-source software kit. The graphical user interface of the software package was developed using a Qt5 cross-platform set of tools and widgets for creating applications. The analysis of the generated binary sequence was performed using a set of statistical tests NIST STS[2].

[2] The National Institute of Standards and Technology, Statistical Test Suite.

Results. The developed software package provides users with a graphical interface for conducting an analysis of a cloud QCD to identify the optimal and most error-resistant set of qubits. The findings from experiments conducted on three cloud quantum computing devices are reported.
Conclusions. The proposed approach, which is constrained by limitations of computing power and duration of access to cloud-based QCD, imposes minimal demands on the productive capabilities of the quantum system. It offers clear and unequivocally interpretable insights into the technical characteristics of a cloud quantum computer, while also being reproducible, easily scalable, and universally applicable.

Keywords: quantum computer, quantum computer device, random number generator, benchmarking

For citation: Korolkov A.V., Kryuchkov A.A. Approach for identifying the optimal set of qubits of quantum computing devices based on a model for generating binary random sequences. *Russian Technological Journal.* 2025;13(6):25–46. https://doi.org/10.32362/2500-316X-2025-13-6-25-46, https://www.elibrary.ru/XEUFSE

Financial disclosure: The authors have no financial or proprietary interest in any material or method mentioned.

The authors declare no conflicts of interest.

ВВЕДЕНИЕ

На протяжении нескольких последних лет квантовые процессоры демонстрируют устойчивый рост собственных вычислительных и технологических показателей. В связи с этим возникает очевидная необходимость в наличии простого и эффективного метода отслеживания и фиксации изменений между промежуточными версиями и этапами развития квантовой вычислительной техники. Одним из таких механизмов (самостоятельно или в составе расширенного набора тестов) может послужить подход к использованию квантовых вычислительных устройств (КВУ) для решения задач генерации случайных чисел (ГСЧ), что может являться надежным и интуитивно понятным механизмом при оценке производительности и надежности исследуемого устройства.

ОЦЕНКА ПРОИЗВОДИТЕЛЬНОСТИ КВУ

В международном научном сообществе на текущий момент не предложен универсальный свод правил по технике проведения анализа вычислительных возможностей КВУ. Однако известно о выполнении подобных работ усилиями Института инженеров и электротехники[3], а также об инициативе Управления перспективных исследований Министерства обороны США[4]. Оба проекта начали реализовываться в 2021 г., и в ближайшее время ожидаются публикации предварительных результатов.

Причина отсутствия единого стандарта объясняется относительной молодостью индустрии квантовых вычислений (первый облачный квантовый компьютер на 1 кубит был предложен в 2016 г.), а также обновлением практически значимых результатов «на ходу»: с каждым годом техники тестирования КВУ корректируются, дополняются и расширяются в зависимости от актуальных показателей и степени соответствия конкретной метрики уровню готовности технологии. К примеру, долгое время используемая метрика «Квантовый объем» (quantum volume) утратила свою значимость в современных устройствах и перестала отражать реальные возможности произвольного КВУ, найдя свое продолжение в обновленных показателях качества и производительности квантового процессора. Более подробно о технологиях и истории становления методов исследования КВУ можно узнать в работах [1–4].

В рамках подтверждения актуальности вопроса и в целях выявления применимости модели ГСЧ в контексте анализа возможностей КВУ определим некоторые ключевые аспекты общепринятых методов оценки их вычислительного потенциала.

Квантовые компьютеры делятся на 4 эпохи технологического развития, на сегодняшний день актуальная из которых имеет наименование noisy intermediate-scale quantum systems (NISQ) – низший уровень в иерархии, что соответствует устройствам с малым количеством кубит на процессоре, предполагает отсутствие кодов коррекции ошибок и подразумевает сильную подверженность квантовой системы помехам, вызванным взаимодействием с окружающей средой.

Второй принципиальный аспект анализа квантового компьютера – технология исполнения. Современные квантовые процессоры могут быть

[3] P7131. Standard for Quantum Computing Performance Metrics & Performance Benchmarking. IEEE. 2021. https://sagroups.ieee.org/7131/. Дата обращения 06.10.12025. / Accessed October 06, 2025.

[4] Quantifying Utility of QC, DARPA. 2021. https://www.darpa.mil/news-events/2021-04-02. Дата обращения 06.10.12025. / Accessed October 06, 2025.

выполнены на основе фотонов, ионов, на сверхпроводниках и нейтральных атомах. «Элементная база» квантового компьютера имеет принципиальное значение при сравнении устройств между собой в рамках различных физических принципов. К примеру, сверхпроводниковые КВУ работают значительно быстрее ионных, что в некоторых случаях предполагает бесперспективность сравнения производительности соответствующих устройств по скорости выполнения квантовой схемы. Однако при фиксации скоростных характеристик в контексте единой физической реализации, пусть и в разных версиях исполнения, сохраняется информативность, демонстрируя степень влияния вносимых в КВУ изменений на скорость обработки квантовой схемы (рис. 1).

Методы исследования КВУ могут различаться в зависимости от области применения: рассматривая систему целиком (например, метрика circuit layer operation per second (CLOPS) [6] – количество обрабатываемых слоев квантовой схемы в секунду), ее отдельные функциональные аспекты (например, метрика error per layer gate (EPLG) [7] – количество ошибок на один слой квантовой схемы), или анализируя самостоятельные элементы на уровне устройства (например, некоторые вентили в связке с конкретными кубитами [8], где к квантовым состояниям применяется определенный набор вентилей для анализа качества узлов квантовой цепи).

Отдельное внимание следует уделить постановке вопроса о сертификации квантовых компьютеров или верификации вычисляемого результата. Главный парадокс заключается в том, что, находясь в классическом мире (класс сложности BPP, bounded-error probabilistic polynomial time – полиномиальное время с ограничением вероятности ошибок), процесс оценки достоверности выполнения квантового алгоритма из квантового мира (класс сложности BQP, bounded-error quantum polynomial time – квантово-полиномиальное время с ограничением вероятности ошибок) становится неоднозначной задачей. Вопрос заключается в том, каким образом можно подтвердить, что программа, отправленная на выполнение квантовому компьютеру, была решена квантовым устройством верно (другими словами, как проверить полученный в ходе квантовых вычислений классический результат). Если в некоторых задачах ответ может быть заранее известен (например, алгоритм Шора [9]) и двоякое толкование итогового результата исключено, до конца непонятно, как следует поступить в тех случаях, когда получаемые вычисления уникальны и не поддаются классической симуляции для сопоставления с ожидаемыми данными.

Оценка производительности и верификация квантовых компьютеров в NISQ-эру должны удовлетворять трем взаимно-дополняющим императивам: качество, скорость, масштабируемость. К примеру, метрика «квантовый объем» утратила свою актуальность именно по причине невозможности соблюдения требования масштабируемости, в связи с чем вендоры квантового оборудования исключили ее из обязательного перечня индикаторов-показателей вычислительного потенциала КВУ.

Завершающим и в то же время фундаментальным аспектом анализа квантовых компьютеров является подход к рассмотрению квантового процессора как устройства в целом. В каноническом виде процесс выполнения квантовой схемы делится на 3 этапа: инициализация квантового регистра, выполнение квантовой схемы, анализ результатов (классическая информация в двоичной форме записи).

Имеющиеся в настоящий момент КВУ для рядовых пользователей доступны исключительно через облачные сервисы. В связи с этим встает вопрос: каким образом независимый исследователь, имея фактический доступ исключительно к результатам работы измерительного аппарата удаленного квантового компьютера (т.е. «черного ящика»), имеет возможность проверить, что в качестве облачного устройства ему не «подсовывается» классический симулятор КВУ?

На первый взгляд, справедливо предположение, что не существует классического устройства (или вычислительного комплекса), способного успешно симулировать работу многоразрядной квантовой программы со значительной глубиной квантовой схемы. Однако, во-первых, в некотором смысле это все же является допущением, а не правилом, во-вторых, отсутствие физического доступа к облачному КВУ и имеющиеся трудности верификации классической информации как результата работы квантового компьютера накладывают ряд ограничений и открывают поле для дальнейших рассуждений (местами, необоснованных фантазий) о характеристиках и свойствах используемого устройства, заявляемого как квантовый компьютер.

Учитывая вышеизложенное, авторы считают целесообразным провести исследование по моделированию генерации случайных двоичных последовательностей на облачных квантовых компьютерах для получения первичной и оперативной информации о производительных мощностях и технических возможностях рассматриваемых устройств.

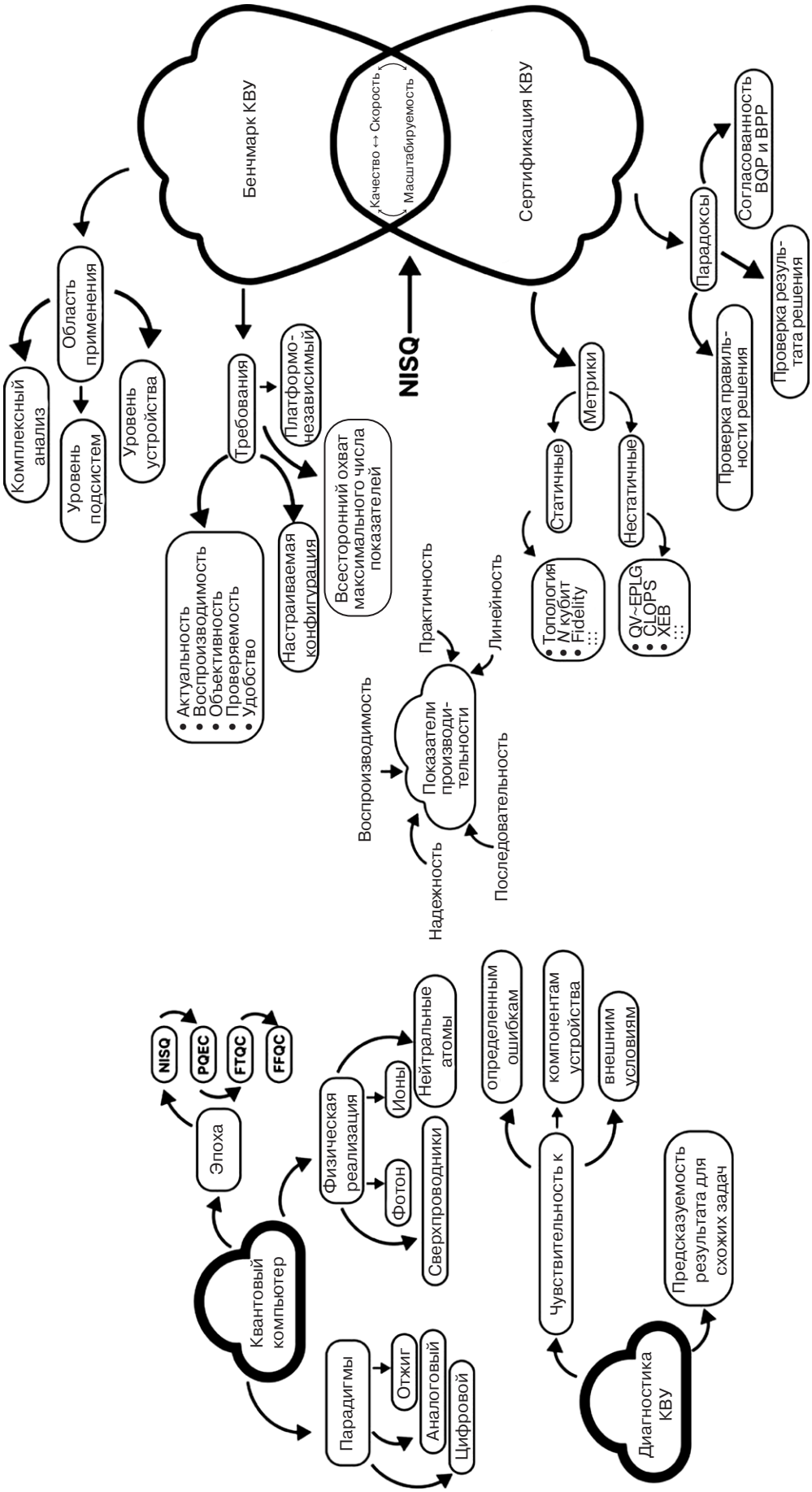

Рис. 1. Структурная схема инструментов оценки производительности КВУ [5]. PQEC (partially quantum error corrected) – частичная коррекция ошибок, возникающих на КВУ; FTQC (fault tolerant quantum computers) – отказоустойчивые КВУ; FFQC (fully functional quantum computers) – полнофункциональные КВУ; XEB (cross-entropy benchmarking) – кросс-энтропийный бенчмаркинг

ПОДХОД К МОДЕЛИРОВАНИЮ ГСЧ НА КВАНТОВОМ КОМПЬЮТЕРЕ

На сегодняшний день качество и достоверность результатов, получаемых в рамках решения прикладных задач современными КВУ, все еще в значительной степени подвержено влиянию окружающей среды, воздействие которой необходимо минимизировать, а также внутренним ошибкам аппаратной реализации оборудования, что обусловлено несовершенством технологии исполнения и суммарной сложностью настройки квантовой системы в целом. Тем не менее, несмотря на все несовершенство современных квантовых компьютеров, авторам видится перспективным проведение анализа вычислительных возможностей и квантовых свойств КВУ в рамках моделирования процесса генерации случайных последовательностей (СП).

Генерация двоичных СП наравне с оценкой технического обеспечения квантового компьютера несет в себе дополнительный практический интерес. Очевидно, что в задачах обеспечения криптографической защиты информации последовательность, сгенерированную на облачном устройстве (независимо от его природы), использовать строго запрещено. Однако проверка самой возможности применения КВУ в задачах ГСЧ может послужить заделом для последующих исследований в период, когда уровень готовности технологий откроет новые возможности по локализации квантовых систем. На текущий момент полученные значения в рамках ГСЧ на облачных КВУ имеет смысл использовать исключительно в исследовательских задачах, например, при моделировании некоторых случайных процессов.

Современные ГСЧ делятся на три основных класса, разделяющие генераторы по технической реализации и способу их исполнения: программные, физические и комбинированные. Программные ГСЧ являются наименее надежной реализацией процесса генерации в виду возможности возникновения периода в выдаваемых псевдослучайных последовательностях (ПСП), а также из-за уязвимости, вызванной наличием инициализирующего вектора, обладание которым может привести к компрометации двоичных данных. Физические и комбинированные ГСЧ зачастую не обладают должным математическим доказательством природы случайности получаемой на выходе информации. Более того, такие генераторы могут быть подвержены условиям окружающей среды, будь то температурный режим, магнитное излучение или влияние радиоволн.

Однако, совершенно иные вводные имеются у квантовых генераторов случайных чисел (КГСЧ), относящихся к классу физических ГСЧ, но имеющих формальное математическое обоснование случайности генерируемых СП. Примеры устройств КГСЧ можно найти в работах [10–12].

Сравнивая портативный КГСЧ и квантовый компьютер в качестве ГСЧ следует отметить, что самостоятельное квантовое устройство генерации СП имеет явное преимущество в виду безопасности генерируемой последовательности (в случае использования КГСЧ в «контролируемой зоне»), но в то же время оно подвержено возможному воздействию окружающей среды, из-за чего выдаваемая битовая строка может качественно терять в свойствах случайности. В свою очередь, облачный квантовый компьютер в идеальных условиях находится в строго изолированной среде, исключающей возникновение побочных шумов и помех, сохраняя физическую природу квантовых вычислений, однако, учитывая удаленное расположение КВУ, ни о какой безопасности в данном случае речи не идет.

Перейдем к описанию моделирования генерации случайного бита классической информации на квантовом компьютере в условиях отсутствия негативного воздействия на КВУ от аппаратного обеспечения и физического окружения устройства. С некоторыми исследованиями в данной предметной области можно ознакомиться в работах [13–16].

Фундаментальной единицей произвольного квантового процессора является кубит, представляющий собой единичный вектор в двумерном комплексном векторном пространстве, базис которого задается ортогональными векторами $|\mathbf{0}\rangle$ и $|\mathbf{1}\rangle$.

$$|\boldsymbol{\psi}\rangle = c_1|\mathbf{0}\rangle + c_2|\mathbf{1}\rangle, \quad (1)$$

где c_1, c_2 – произвольные комплексные числа, амплитуды вероятностей квантового состояния такие, что:

$$|c_1|^2 + |c_2|^2 = 1. \quad (2)$$

Для получения случайного бита, оперируя одним кубитом квантового процессора, необходимо и достаточно установить единичный вектор в состояние суперпозиции, когда по результатам измерения вероятность получения «0» и «1» будет равняться 0.5. Таким образом, к квантовому состоянию следует применить преобразование Уолша – Адамара, описываемое следующей матрицей:

$$\mathbf{H} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}. \quad (3)$$

В результате применения вентиля Адамара к одиночному кубиту будет получена суперпозиция квантового состояния, которая задается следующим выражением:

$$\mathbf{H}:|\mathbf{0}\rangle \to \frac{1}{\sqrt{2}}\left(|\mathbf{0}\rangle + |\mathbf{1}\rangle\right),$$
$$\mathbf{H}:|\mathbf{1}\rangle \to \frac{1}{\sqrt{2}}\left(|\mathbf{0}\rangle - |\mathbf{1}\rangle\right). \quad (4)$$

Как можно видеть из (4), не имеет значения, с какого состояния начинается моделирование ГСЧ, независимо от того, находится кубит в состоянии $|\mathbf{0}\rangle$, либо $|\mathbf{1}\rangle$. В результате будет получено состояние суперпозиции, равновероятно обращающее после измерения квантовый бит в классический – «0» или «1». Для того чтобы получить СП заданной длины, необходимо запустить операцию (4) в цикле на необходимое количество тактов с последующим сохранением результатов в единую двоичную битовую строку.

Предложенная модель КГСЧ представляет собой идеализированный процесс генерации СП, проводимый в «безупречных» условиях, где в результате должна быть получена СП с равновероятным распределением «0» и «1». Однако на практике воссоздать такие условия, по крайней мере на сегодняшний день, не представляется возможным. В первую очередь это обусловлено технологическим несовершенством квантового оборудования, находящегося в распоряжении производителей квантовых процессоров в эпоху NISQ-устройств.

Заметим, что преодолению возникающих технических ограничений, вызванных несовершенством аппаратной части и внешним воздействием окружающей среды, уделяется пристальное внимание со стороны разработчиков квантового оборудования. На сегодняшний день в целях улучшения качества работы квантовых алгоритмов предлагается использовать коды коррекции ошибок, которые подразумевают под собой использование нескольких *физических* кубитов в качестве одного *логического*.

К примеру, работая с одним логическим кубитом, построенным на трех физических, при передаче квантового состояния $|\mathbf{0}\rangle$ получатель должен принять закодированное состояние $|\mathbf{000}\rangle$ (кодовое слово). В случае, если один из битов был инвертирован (bit-flip), например, первый – $|\mathbf{100}\rangle$, пользователь обнаружит ошибку. Если же количество искаженных бит (bit-flip) будет больше двух, выявление несоответствия в итоговом результате не представляется возможным. Таким образом, в приведенном случае необходимо внимательно подходить к выбору кодового расстояния $d = 2t + 1$, где d – количество ошибок, которое не может быть обнаружено, t – количество детектируемых ошибок.

В настоящее время к наиболее известным кодам коррекции квантовых ошибок относят следующие[5]: код повторений, код Шора, поверхностный код, код Стина (Steane), код Хастингса (Hastings – Haah).

В то же время, в контексте поставленной задачи применение кодов коррекции ошибок нецелесообразно, т.к. для генерации (предполагаемо) истинно СП необходимо работать с квантовыми состояниями непосредственно на физическом уровне.

Современные квантовые компьютеры имеют ряд параметров, по которым возможно предварительно оценить вычислительные возможности и технические характеристики исследуемого устройства. В табл. 1 представлены параметры, свойственные квантовым процессорам, реализованным на основе сверхпроводниковой технологии (в дальнейшем эксперименты будут проводится на квантовых

Таблица 1. Влияние параметров сверхпроводящих КВУ на этап выполнения квантовой схемы

Этап выполнения квантовой схемы	Параметр КВУ											
	T_1	T_2	Frequency	Anharmonicity	Readout length	Readout error	meas0 prep1	meas1 prep0	(ID) error	(Pauli-X) error	(sx) error	ECR error
Инициализация кубит	–	–	–	–	–	–	+	+	–	–	–	–
Выполнение квантовой схемы	+	+	+	+	–	–	–	–	+	+	+	+
Измерение регистра	–	–	–	–	+	+	–	–	–	–	–	–

Примечание: T_1, T_2 – время релаксации и дефазировки состояний; Frequency, Anharmonicity – частота, ангармоника (разница в энергии между первым и вторым возбужденными состояниями кубита, выраженная в Гц); Readout error/length – ошибка/время чтения кубита; meas0/1 prep1/0 – ошибка инициализации; (ID) error, (Pauli-X) error, (sx) error – ошибки вентиля инициализации, инверсии, суперпозиции кубита; ECR error – ошибка двухкубитного вентиля.

[5] Introduction to quantum error correction. Microsoft Quantum Azure. 2024. https://learn.microsoft.com/en-us/azure/quantum/concepts-error-correction. Дата обращения 06.10.12025. / Accessed October 06, 2025.

процессорах компании IBM, реализованных на сверхпроводниках[6]).

Значения из табл. 1 не распространяются целиком на все три упомянутых ранее этапа выполнения программы на квантовом компьютере, а оказывают свое влияние лишь на определенном промежутке работы квантовой схемы на удаленном устройстве. Более того, не все из них должны учитываться при предварительной оценке качества исследуемого кубита. Для того чтобы понимать, какие из параметров могут быть опущены, следует построить квантовую схему, из которой станет очевидно, какой набор характеристик по отношению к выбранным кубитам должен быть взят в расчет.

Генератор СП на квантовом компьютере может быть реализован так, как это показано на рис. 2. В то время как рис. 2а отображает квантовую схему, изначально запрограммированную пользователем, рис. 2б отображает ту же схему после процесса компиляции программы и разложения ее на новую в рамках базовых вентилей («native gates»), свойственных тому квантовому компьютеру, на котором происходит моделирование и запуск пользовательской программы. К примеру, та же схема, выполненная на КВУ иной физической природы с другим набором базовых вентилей, может принципиально отличаться от искомой.

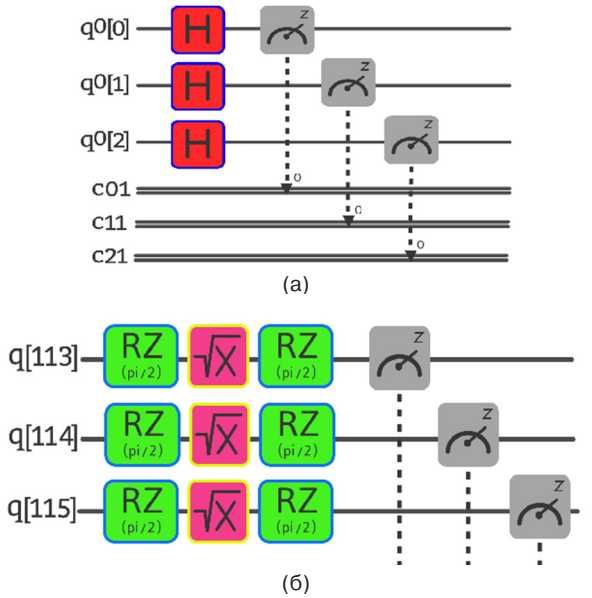

Рис. 2. Схема КГСЧ на трех кубитах для сверхпроводящего КВУ: (а) представление на высоком уровне, (б) разложение на базовые вентили КВУ (низкий уровень представления). q0[0], q0[1], q0[2], q[113], q[114], q[115] – кубит; c11, c12, c21 — классический бит; H – вентили Адамара; «спидометр» – операция измерения кубита; RZ – вращение квантового состояния (на угол π/2); $\sqrt{X}$ – одна из составляющих операций Адамара [17]

[6] IBM Quantum Platform. https://quantum.ibm.com/. Дата обращения 15.05.2025. / Accessed May 15, 2025.

Учитывая квантовую схему после компиляции (рис. 2б), а также имеющиеся параметры КВУ (табл. 1), можно сделать вывод, что параметрами, которые необходимо брать в расчет, будут являться следующие: T_1, T_2, Readout error, (sx) error.

Забегая вперед, скажем, что характеристики Frequency, Anharmonicity, Readout length опускаются умышленно по причине малого отличия наблюдаемых значений для всего набора кубит, который использовался в рамках исследовательских экспериментов. Параметры meas0 prep1 и meas1 prer0 в контексте задачи не имеют смысла – вентиль «H» применяется к кубитам на «холостом ходу», без предварительной инициализации. Более того, в соответствии с (4) предполагается, что результат работы программируемой схемы не зависит от исходного состояния кубита[7]. Наконец, из оставшегося блока ошибок, влияющих на задействованные кубиты, актуальным будет только (sx) error, что следует из схемы на рис. 2б. Вентиль, отвечающий за поворот квантового состояния (rz), по сведениям производителя используемых облачных КВУ, имеет нулевое значение ошибки и также не учитывается.

Сформулировав модель генерации СП и определив, на какие параметры облачного КВУ следует обратить внимание при интерпретации результатов, проведем практическую серию экспериментов КГСЧ на облачном квантовом компьютере.

ЭКСПЕРИМЕНТАЛЬНАЯ РЕАЛИЗАЦИЯ КГСЧ НА ОБЛАЧНОМ КВУ

Для выполнения серии опытов использовались квантовые компьютеры IBM, предоставленные пользователям в свободном доступе через облачные сервисы компании.

В целях повышения эффективности, автономности, вариативности и удобства работы с квантовыми устройствами авторами разработано приложение с использованием библиотеки с открытым исходным кодом Qiskit, реализованное с помощью графической оболочки фреймворка Qt5. Внешний вид главного окна программы, получившей название *QIS* (*Quantum Information Security*) [18], представлен на рис. 3.

При запуске программы для установления удаленного соединения с облачным КВУ (область 1) оператору необходимо ввести инициализирующие данные, указав персональный API[8]-токен, уникальный для каждого пользователя. Следующий

[7] Как правило, по умолчанию квантовый регистр «сброшен» в состояние |00...0⟩. [As a rule, the quantum register is “reset” to the state |00...0⟩ by default.]

[8] Application programming interface – программный интерфейс приложений.

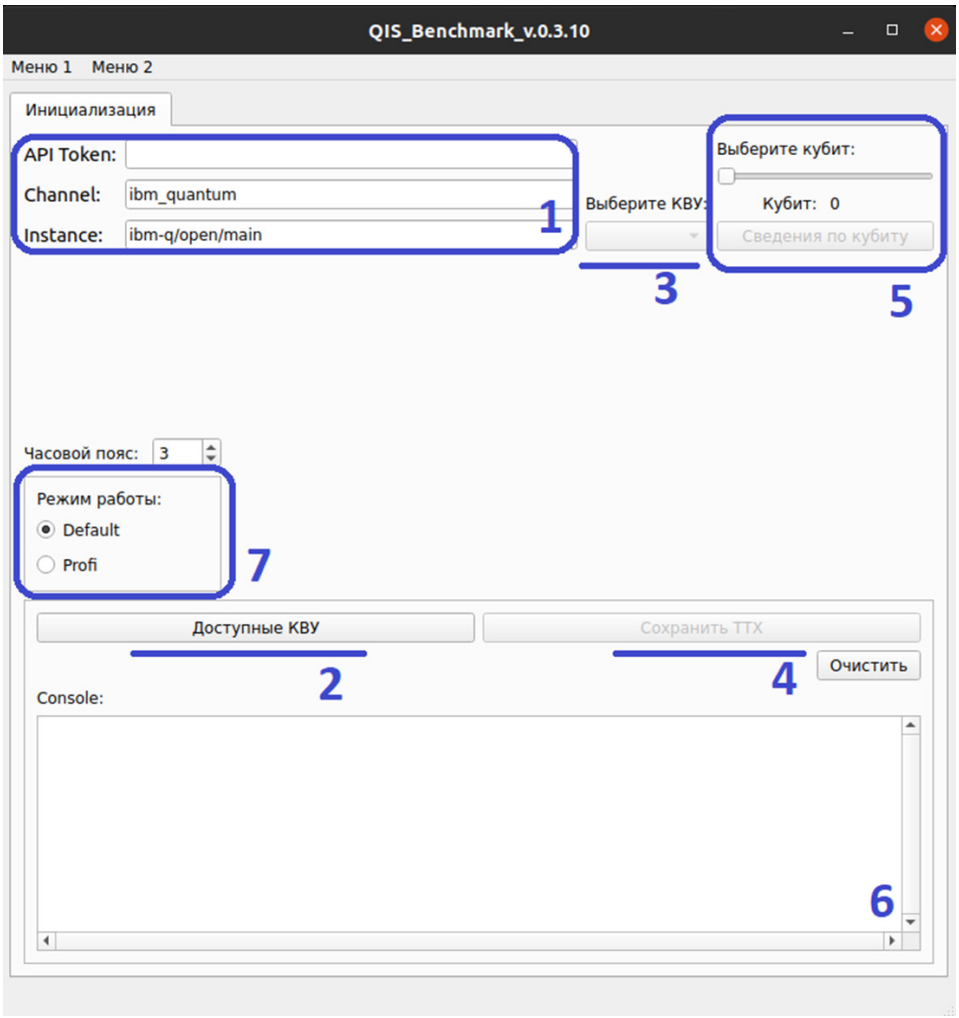

Рис. 3. Главное окно программы *QIS*. ТТХ – тактико-технические характеристики

шаг – получение информации о доступных облачных КВУ (область 2). На сегодняшний день компания IBM предлагает возможность запуска квантовых схем на 12 устройствах, 9 из которых являются коммерческими. В связи с этим, при отсутствии платной подписки проводить исследования возможно только на 3 облачных системах. После получения информации об имеющихся в распоряжении пользователя КВУ будет заполнен выпадающий список (область 3) и активирована возможность получения общей (область 4) и детальной (область 5) информации по выбранному КВУ или конкретному кубиту, соответственно.

Текстовое окно предназначено для отражения хода выполнения программы (область 6). Выбор режима работы (область 7) для менее подготовленных пользователей призван упростить работу как с самим приложением, так и с облачным квантовым компьютером.

После перехода в режим Profi программа раскрывает дополнительные окна, внешний вид которых представлен на рис. 4.

Режим INIT-IDLE[9] (рис. 4, слева) преследует цель «точечного» исследования кубит. После выбора КВУ (область 3) пользователь определяет, какие кубиты следует задействовать (область 4), к каким состояниям необходимо применить вентиль инициализации (область 5) и вентиль Адамара (область 6). Следующим шагом задаются инструкции для квантового компьютера, и схема отправляется на выполнение (область 7). Дополнительно реализована возможность скачивания результатов программы по идентификатору JobID в случае, если у пользователя отсутствует возможность дождаться завершения работы КВУ в режиме онлайн (область 8). Текстовое окно отображает ход выполнения программы (область 9).

[9] INIT – Initialization (инициализация); IDLE – на «холостом» ходу (инициализация). Режим «INIT-IDLE» в данной работе рассмотрен не будет. [INIT is initialization; IDLE stands for on “idle” (initialization). The “INIT–IDLE” mode is not considered in the paper.]

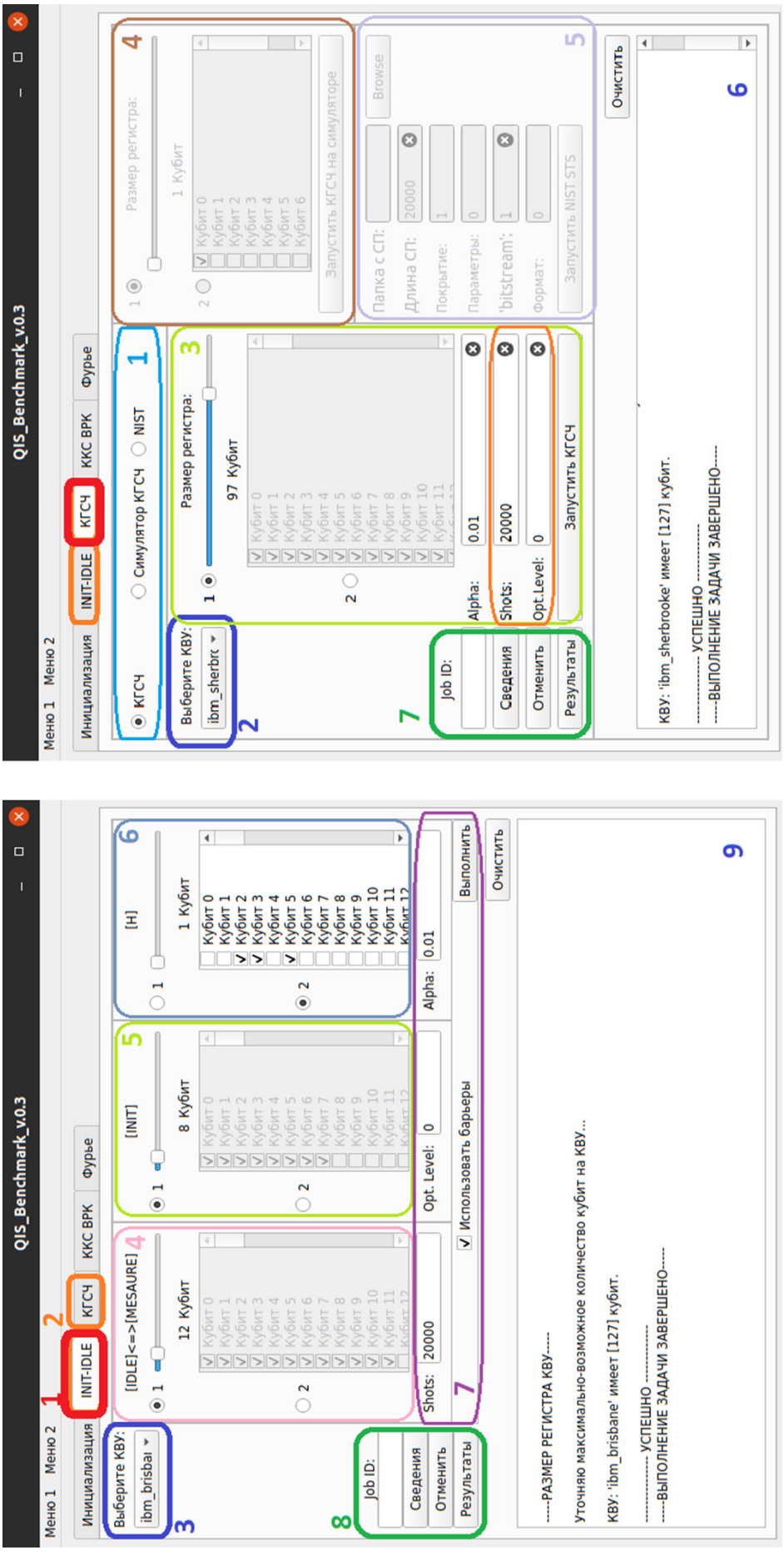

Рис. 4. Интерфейс вкладок INIT-IDLE и КГСЧ приложения *QISs*. ККС ВРК - квантовые криптографические системы выработки и распределения ключа; NIST (National Institute of Standards and Technology) – Национальный институт стандартов и технологий США

Режим КГСЧ (рис. 4, справа) предоставляет несколько функциональных возможностей (область 1), где выбор облачного КВУ нужен только для блока по настройке КГСЧ (область 3). В качестве тренировки процесса генерации квантовой схемы и анализа информации имеется возможность выполнения КГСЧ на симуляторе квантового компьютера (область 4). Область 5 отвечает за проведение тестирования сгенерированных СП и ПСП на предмет наличия статистической зависимости в двоичных строках. Вкладка КГСЧ также предполагает возможность сохранения полученных результатов в режиме офлайн (область 7). Все этапы работы приложения отображаются в текстовом поле 6.

Отдельно отметим один из наиболее важных параметров – Alpha (уровень значимости). При ГСЧ последовательность с каждого кубита исследуется на предмет соответствия полученного распределения «0» и «1» равномерному закону. В этих целях приложение проводит частотный побитовый тест, входящий в набор статистических тестов NIST STS[10] по исследованию бинарных последовательностей[11]. В результате тестирования пользователь получает рассчитанное статистическими методами значение P_{value}, находящееся в диапазоне от 0 (наблюдается сильное смещение) до 1 (распределение «0» и «1» равновероятно). Отметим, что не всегда значение P_{value} принимает граничные положения, в результате чего решение о случайности (равномерности распределения) СП отдается на усмотрение пользователя, который самостоятельно выбирает уровень значимости Alpha, используемый для сравнения со статистическими метриками.

В документации к тестам NIST STS рекомендуется использовать Alpha на уровне 0.001–0.01 – превышение значением P_{value} уровня значимости ($P_{\text{value}} > \alpha$) предполагает, что полученная последовательность случайна с уровнем доверия 99.9% и 99% соответственно. Выбранное значение Alpha отвечает за ошибки 1-го рода – ложноположительное заключение и ошибочное отклонение нулевой гипотезы. Так, при α = 0.01 одна из 100 СП будет неверно отклонена.

В программе *QISs* частотный побитовый тест используется для просеивания квантовых состояний на два множества: «плохие» и «хорошие» кубиты, где пользователь для классификации квантовых состояний определяет граничное значение «Alpha». Разделение кубит, пусть и весьма условное, однако в некоторых случаях – наглядное и необходимое.

Для проведения частотного побитового теста двоичной последовательности $\{x\}_{i=1}^{n}$ подсчитывается наблюдаемая статистика количества «0» и «1» по следующему правилу:

$$s_{\text{obs}} = \frac{|S_n|}{\sqrt{n}}, \tag{5}$$

где при $X_i = 2x_i - 1$:

$$S_n = \sum_{i=1}^{n} X_i. \tag{6}$$

По результатам найденного значения через дополнительную функцию ошибок, имеющую вид:

$$\operatorname{erfc}(x) = \frac{2}{\sqrt{\pi}} \int_x^{\infty} \mathrm{e}^{-t^2}\, dt, \tag{7}$$

вычисляется значение P_{value}:

$$P_{\text{value}} = \operatorname{erfc}\left(\frac{s_{\text{obs}}}{\sqrt{2}}\right). \tag{8}$$

Если рассчитанное значение P_{value} оказывается меньше выбранного пользователем уровня значимости Alpha, заключается, что СП не удовлетворяет условию случайности[12]. В противном случае, когда P_{value} больше уровня значимости, СП считается качественной, а кубит – устойчивым и пригодным для его применения в задачах ГСЧ.

Представив описание и базовые функциональные возможности программы *QISs*, а также определив, по какому принципу будет осуществляться выявление устойчивых и надежных кубит из общего числа квантовых состояний регистра КВУ, выполним генерацию СП на облачном квантовом компьютере. Для этого:

1. На вкладке КГСЧ в выпадающем списке выберем КВУ ibm_brisbane и дождемся, когда с облачным устройством будет установлена связь.
2. Отметим весь квантовый регистр КВУ с помощью элемента интерфейса slider, ibm_brisbane имеет 127 кубит. Выберем все 127 квантовых состояний для КГСЧ.
3. Присвоим уровню значимости «Alpha» значение 0.01.

[10] The National Institute of Standards and Technology, Statistical Test Suite – Национальный институт стандартов и технологий США, набор статистических тестов.

[11] NIST SP 800-22. https://csrc.nist.gov/projects/random-bit-generation/documentation-and-software. Дата обращения 15.05.2025. / Accessed May 15, 2025.

[12] Очевидно, что частотный тест является необходимым, но недостаточным условием случайности СП. [The frequency test is clearly an essential step in assessing the randomness of the RS, though on its own, it remains insufficient to fully establish randomness.]

4. Зададим количество повторений квантовой схемы в размере 20000 (предельное доступное на момент проведения исследований). Таким образом, с каждого кубита будет получена СП длиной $2 \cdot 10^4$ бит. Суммарная длина возможного ключа составит $254 \cdot 10^4$ бит, что приблизительно равняется ~0.3 МБ (из расчета 127 кубит на КВУ с максимальным числом запусков квантовой схемы $2 \cdot 10^4$).
5. Уровень оптимизации квантовой схемы для поставленной задачи не имеет значения. Оставим параметр равным 0.
6. Все настройки выполнены. Запустим процесс КГСЧ.

АНАЛИЗ И ИНТЕРПРЕТАЦИЯ РЕЗУЛЬТАТОВ

Этап 1. Сбор статистики

После завершения работы квантового компьютера в домашней директории пользователя будут сохранены полученные результаты (рис. 5).

Каталоги под цифрами «1» и «2» хранят файлы со СП с каждого кубита, но уже после просеивания квантовых состояний на «хорошие» и «плохие». В папках «3» и «4» содержатся файлы, полученные в результате конкатенации всех СП из каталогов «1» и «2» соответственно. Замысел авторов заключается в получении итогового случайного двоичного ключа с кубит, которые были определены как устойчивые, пригодные для реализации процесса КГСЧ. Финальный «плохой» ключ создается для возможности оценки и сравнения полученных ключей, а, следовательно, и кубит, друг с другом. На рис. 5 снизу представлено содержимое файла с итоговой статистикой отдельного эксперимента, подсчитанной для «хороших» кубит КВУ.

Учитывая вероятностную природу вычислительного процесса квантовых компьютеров очевидно, что одного запуска может быть недостаточно. В связи с этим программа *QISs* предполагает накопление статистической информации о выполненных ранее проектах. На рис. 6 представлены собранные сведения по запуску КГСЧ на двух КВУ компании IBM.

Такой подход призван предоставить возможность наглядного прослеживания изменения в количестве и качестве кубит квантового регистра облачного устройства. Однако в данном случае нужно быть осторожным с интерпретацией результатов. В некоторых случаях незначительные колебания на считанные значения в соотношении «0» и «1» могут автоматически присвоить кубиту статус «ненадежный» (ложное срабатывание), в то время как на самом деле ориентировочное количество нулей и единиц практически не изменилось. В связи с этим нужно понимать, какую именно цель преследует пользователь:

1. Получение случайного двоичного ключа с наилучшими характеристиками исходя из возможностей КВУ (строгие требования к Alpha, увеличение параметра в зависимости от качества генерируемой СП).

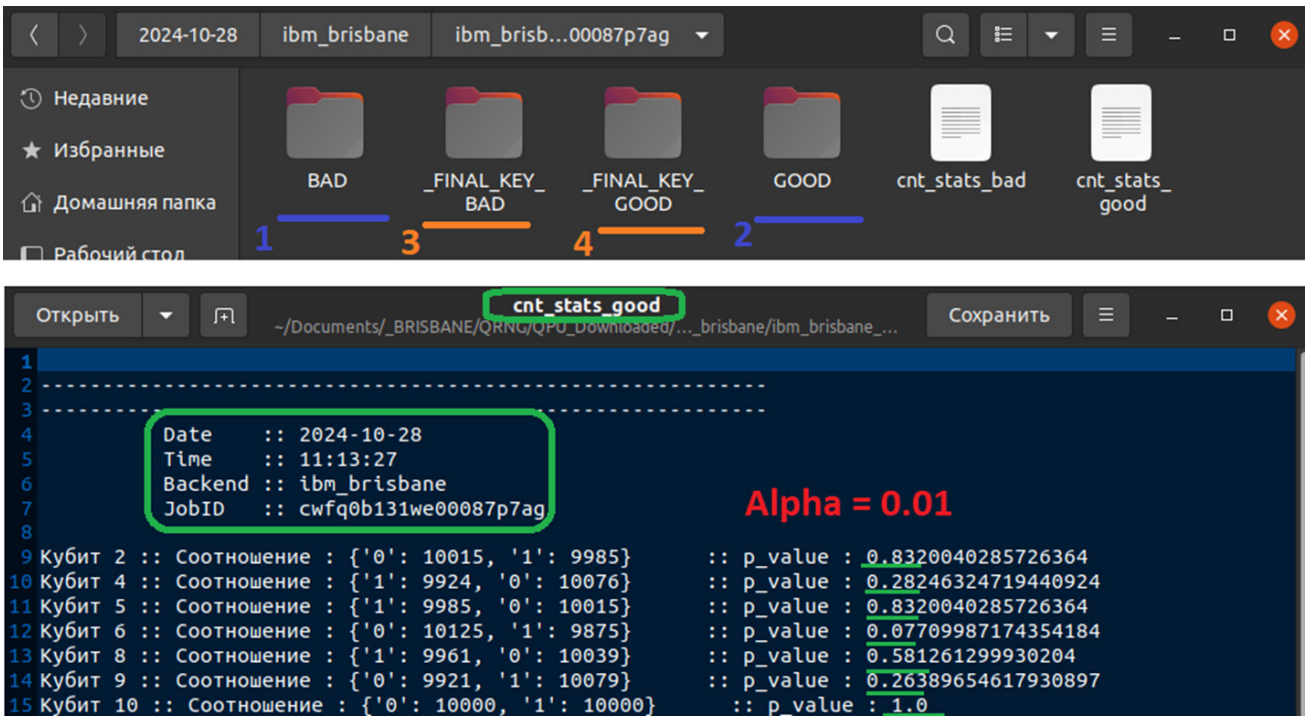

Рис. 5. Результаты работы программы *QISs* (режим КГСЧ)

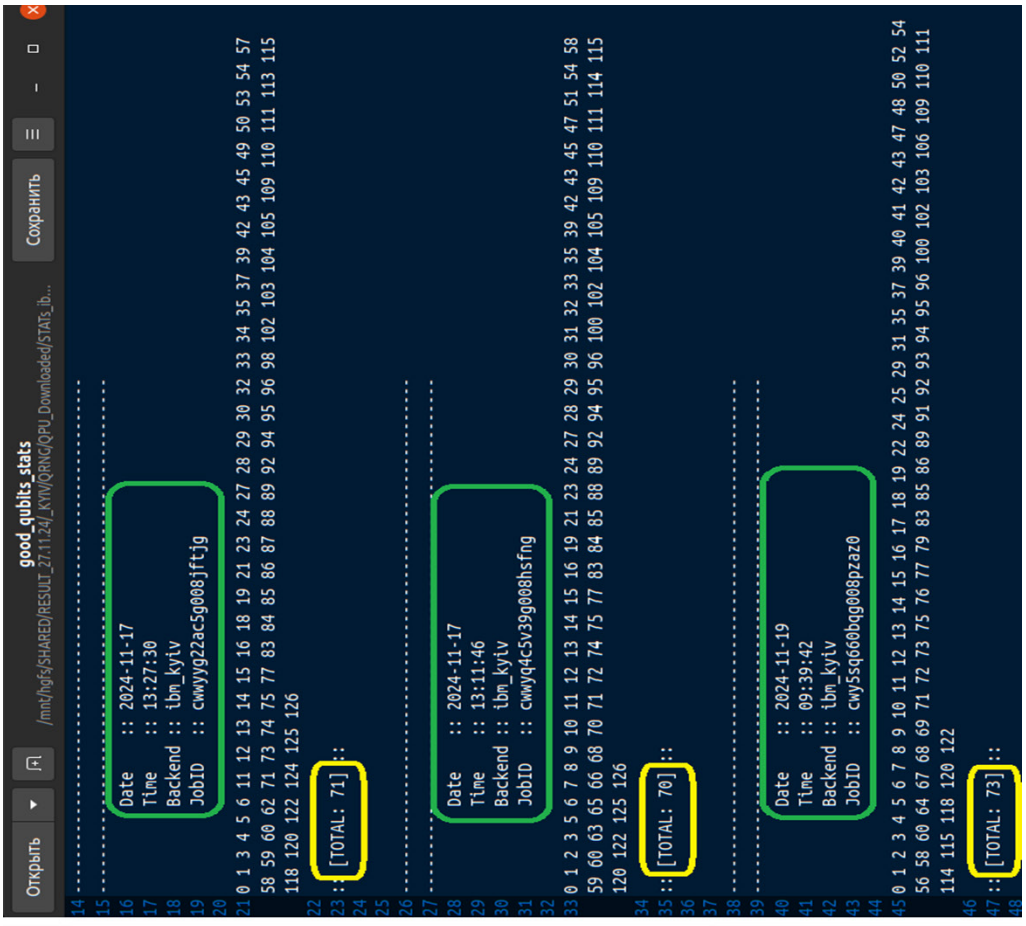

Рис. 6. Статистика по кубитам трех облачных КВУ в задачах КГСЧ

2. Оценка квантового регистра КВУ в целях определения наиболее стабильных и устойчивых кубит для выбора оптимального набора квантовых состояний в рамках будущих экспериментов (лояльные требования к Alpha, допускается уменьшение до необходимого уровня).

С учетом вышесказанного можно заключить: во-первых, необходимо тщательно продумывать, какой уровень значимости следует выбрать для просеивания кубит по частотному признаку; во-вторых, важно всегда сверяться с итоговой статистикой отдельного эксперимента (рис. 5), где прописаны все значения «0» и «1» по каждому кубиту. Возможно, в некоторых случаях понадобиться «ослабить» параметр Alpha. Но следует быть аккуратным – при желании получить надежную СП такой подход может привести к «набеганию» незначительных отклонений с каждого кубита в существенные разрывы между «0» и «1» в итоговом ключе после конкатенации полученных файлов.

Этап 2. Корреляционный анализ

Без проведения предварительного корреляционного анализа полученных результатов даже с «хороших» кубит не рекомендуется проводить конкатенацию сгенерированных файлов с двоичными последовательностями.

В некотором смысле, отправляя схему по реализации КГСЧ на квантовый компьютер, можно заключить, что сам КВУ не является самостоятельным ГСЧ – в нашем случае весь квантовый компьютер делится на множество более мелких генераторов СП, в качестве которых выступают отдельные кубиты облачного устройства.

Тогда возникает закономерный вопрос: можно ли в таком случае считать каждый кубит независимым источником случайных данных? Ответ напрямую влияет на то, имеются ли серьезные обоснования в пользу положительного решения о выполнении объединения малых СП друг с другом в один итоговый ключ с двух и более кубит.

Цель проверки на корреляцию СП – определить, являются ли выбранные кубиты независимыми источниками случайных чисел как по отношению к самим себе, так и в сопоставлении с другими состояниями квантового регистра.

Для двух двоичных СП $\{x\}_{i=1}^{n}, \{z\}_{i=1}^{n}$ длины $n \in \mathbb{N}$ корреляционная функция сгенерированных последовательностей задается выражением:

$$F_{\mathrm{corr}(i)} = \frac{1}{n}\sum_{j=1}^{n} s_j,\ i = (0, n), \qquad (9)$$

где $s_j = 1$, если $\overline{x \oplus z(i)} = 1$; и $s_j = -1$, в случае $\overline{x \oplus z(i)} = 0$. Другими словами, s_j выполняет побитовое сложение по модулю 2 двух последовательностей, но в контексте сравнения двоичных строк анализ выполняется с циклическим сдвигом. Инверсия применяется в целях наглядности графической интерпретации результатов – для получения единицы в случае сравнения двух идентичных последовательностей.

На данный момент текущая версия приложения *QISs* не содержит автоматического предварительного анализа получаемых СП на корреляцию, однако, на конференции «РАДИОИНФОКОМ», прошедшей в ноябре 2024 г. [19], были представлены результаты такого анализа. Итог предварительных исследований показал, что корреляция между «хорошими» кубитами не превышает порядкового значения в 10^{-3}, в то время как кубиты, генерирующие менее устойчивые и надежные последовательности, имели определенное смещение функции корреляции в пределах, достигающих значений в $4 \cdot 10^{-2}$.

Этап 3. Проверка на статистическую независимость

Наконец, завершающим этапом проверки сгенерированных СП является их исследование на статистическую независимость. Одним из возможных инструментов такой проверки может выступить набор тестов NIST STS, который включен в программу *QISs* для автономной и настраиваемой пользователем проверки СП (рис. 4, справа, область 5).

Непосредственный интерес представляет анализ итоговой СП, полученной в результате объединения двоичных строк с «хороших» кубит. Однако исследование отдельно взятой последовательности не всегда является информативным, в связи с чем более закономерным будет сравнение итоговых последовательностей, полученных за определенный промежуток времени, что позволит проследить особенности в работе квантового устройства на дистанции (длина итогового ключа, количество (не)пройденных тестов, …).

На рис. 7 представлены данные, полученные при анализе СП с квантового компьютера ibm_brisbane с разницей в один месяц.

В ходе экспериментов количество устойчивых кубит незначительно изменялось, в то же время на начало и конец месяца их количество сохранилось на уровне 79 кубит. Результаты прохождения тестов не претерпели существенных изменений за исключением теста на длину последовательности подряд идущих «1», который был успешно пройден во втором случае.

Аналогичные исследования проведены для КВУ ibm_kyvi с разницей в 2 недели (рис. 8а) и ibm_sherbrooke с интервалом в 7 дней (рис. 8б).

Рис. 7. Результаты проверки итоговой СП с КВУ ibm_brisbane

05.11.24 // 1.180.000 бит

RESULTS FOR THE UNIFORMITY OF P-VALUES AND THE PROPORTION OF PASSING SEQUENCES

generator is </home/amd/Documents/QISs/NIST/ResultTest_2024-11-29_16:24:08/KEY.txt>

C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	P-VALUE	PROPORTION	STATISTICAL TEST
9	0	1	0	0	0	0	0	0	0	0.000000 *	8/10	Frequency
5	2	0	0	1	0	1	1	0	0	0.008879	10/10	BlockFrequency
8	1	1	0	0	0	0	0	0	0	0.000000 *	8/10	CumulativeSums
8	1	0	1	0	0	0	0	0	0	0.000000 *	7/10 *	CumulativeSums
3	4	0	1	0	0	1	1	0	0	0.035174	10/10	Runs
2	1	0	0	0	1	2	0	2	2	0.534146	9/10	LongestRun
1	0	0	1	1	3	0	1	1	2	0.534146	10/10	Rank
2	2	1	0	2	0	0	0	2	1	0.534146	9/10	FFT
2	2	1	1	1	1	2	0	0	0	0.739918	9/10	NonOverlappingTemplate
1	1	0	2	2	1	1	0	1	1	0.911413	10/10	NonOverlappingTemplate
4	1	0	1	1	0	1	0	0	2	0.122325	10/10	NonOverlappingTemplate
1	0	2	1	2	0	1	0	2	1	0.739918	10/10	NonOverlappingTemplate

24.11.24 // 1.280.000 бит

RESULTS FOR THE UNIFORMITY OF P-VALUES AND THE PROPORTION OF PASSING SEQUENCES

generator is </home/amd/Documents/QISs/NIST/ResultTest_2024-11-29_16:24:58/KEY.txt>

C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	P-VALUE	PROPORTION	STATISTICAL TEST
7	1	2	0	0	0	0	0	0	0	0.000001 *	4/10 *	Frequency
3	1	1	1	0	1	1	1	0	1	0.739918	9/10	BlockFrequency
7	0	1	1	1	0	0	0	0	0	0.000003 *	4/10 *	CumulativeSums
7	2	0	1	0	0	0	0	0	0	0.000001 *	4/10 *	CumulativeSums
5	1	0	0	0	1	1	0	0	2	0.008879	8/10	Runs
1	0	2	1	0	1	1	3	1	0	0.534146	10/10	LongestRun
0	3	0	1	1	0	1	2	1	1	0.534146	10/10	Rank
2	2	0	0	0	2	0	0	3	1	0.213309	10/10	FFT
1	1	0	1	0	3	2	0	1	1	0.534146	10/10	NonOverlappingTemplate
3	0	2	1	2	0	0	0	1	1	0.350485	10/10	NonOverlappingTemplate
4	1	2	0	1	1	0	1	0	0	0.122325	9/10	NonOverlappingTemplate
0	1	0	1	3	1	0	2	0	2	0.350485	10/10	NonOverlappingTemplate

(а)

06.11.24 // 1.040.000 бит

RESULTS FOR THE UNIFORMITY OF P-VALUES AND THE PROPORTION OF PASSING SEQUENCES

generator is </home/amd/Documents/QISs/NIST/ResultTest_2024-11-29_16:22:32/KEY.txt>

C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	P-VALUE	PROPORTION	STATISTICAL TEST
7	2	0	0	1	0	0	0	0	0	0.000001 *	7/10 *	Frequency
0	3	2	0	1	1	2	0	0	1	0.350485	10/10	BlockFrequency
8	1	1	0	0	0	0	0	0	0	0.000000 *	7/10 *	CumulativeSums
8	1	1	0	0	0	0	0	0	0	0.000000 *	7/10 *	CumulativeSums
0	1	2	3	0	1	1	0	1	1	0.534146	10/10	Runs
0	2	0	0	3	3	0	1	0	1	0.122325	10/10	LongestRun
1	2	1	0	0	1	1	1	3	0	0.534146	10/10	Rank
1	1	0	0	0	2	2	2	1	1	0.739918	10/10	FFT
1	1	1	3	1	1	0	1	1	0	0.739918	10/10	NonOverlappingTemplate
3	1	0	2	1	0	0	1	1	1	0.534146	10/10	NonOverlappingTemplate
2	1	0	2	2	0	1	1	1	0	0.739918	9/10	NonOverlappingTemplate
2	1	1	2	1	1	0	0	1	1	0.911413	9/10	NonOverlappingTemplate

12.11.24 // 1.040.000 бит

RESULTS FOR THE UNIFORMITY OF P-VALUES AND THE PROPORTION OF PASSING SEQUENCES

generator is </home/amd/Documents/QISs/NIST/ResultTest_2024-11-29_16:23:19/KEY.txt>

C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	P-VALUE	PROPORTION	STATISTICAL TEST
7	1	1	0	0	1	0	0	0	0	0.000003 *	5/10 *	Frequency
2	1	1	0	1	0	2	0	2	1	0.739918	10/10	BlockFrequency
7	0	0	1	1	0	0	1	0	0	0.000003 *	5/10 *	CumulativeSums
9	0	0	1	0	0	0	0	0	0	0.000000 *	6/10 *	CumulativeSums
1	1	0	0	0	1	3	1	2	1	0.534146	9/10	Runs
1	1	2	1	0	1	0	2	2	0	0.739918	10/10	LongestRun
2	0	1	0	4	1	2	0	0	0	0.066882	10/10	Rank
2	1	2	0	0	1	0	3	0	1	0.350485	10/10	FFT
2	5	1	0	1	0	0	1	0	0	0.008879	10/10	NonOverlappingTemplate
1	2	1	1	0	1	1	1	1	1	0.991468	10/10	NonOverlappingTemplate
1	1	2	1	2	0	1	0	0	2	0.739918	10/10	NonOverlappingTemplate
0	1	3	0	2	1	0	2	1	0	0.350485	10/10	NonOverlappingTemplate

(б)

Рис. 8. Результаты проверки итоговой СП с КВУ: (а) ibm_ kyvi, (б) ibm_sherbrooke

Таблица 2. Результаты выполнения исследований процесса КГСЧ на облачных КВУ

Дата	КВУ	Кол-во «хороших» кубит / длина СП	Непройденные тесты NIST STS[13]	Время работы схемы, с	Лучшее / Худшее соотношение «0»–«1» на всем регистре КВУ
28.10.2024	ibm_brisbane	79 / $158 \cdot 10^4$	«Runs» 1 тест «RandomExcursions» 8 тестов «RandomExcursionsVariant» 18 тестов	7	10.000–10.000 / 12.684–7.316
26.11.2024	ibm_brisbane	79 / $158 \cdot 10^4$	«RandomExcursions» 8 тестов «RandomExcursionsVariant» 18 тестов	8	9.999–10.001 / 7.498–12.502
05.11.2024	ibm_kyvi	59 / $118 \cdot 10^4$	«Frequency» 1 тест «CumulativeSums» 2 теста	13	9.998–10.002 / 13.029–6.971
24.11.2024	ibm_kyvi	64 / $128 \cdot 10^4$	«Frequency» 1 тест «CumulativeSums» 2 теста «RandomExcursions» 8 тестов «RandomExcursionsVariant» 18 тестов	14	9.999–10.001 / 15.143–4.857
06.11.2024	ibm_sherbrooke	52 / $104 \cdot 10^4$	«Frequency» 1 тест «CumulativeSums» 2 теста «RandomExcursions» 8 тестов «RandomExcursionsVariant» 18 тестов	9	9.997–10.003 / 13.404–6.596
12.11.2024	ibm_sherbrooke	52 / $104 \cdot 10^4$	«Frequency» 1 тест «CumulativeSums» 2 теста «RandomExcursions» 8 тестов «RandomExcursionsVariant» 18 тестов	8	9.984–10.016 / 12.596–7.404

Характер прохождения тестов для двух приведенных на рис. 8 КВУ заслуживает отдельного внимания. В то время как по отдельности СП с каждого «хорошего» кубита выбранного КВУ длиной $2 \cdot 10^4$ бит успешно проходят частотный побитовый тест, в обоих случаях конкатенация этих строк в итоговые СП (размером немногим больше 0.1 МБ) проваливают идентичные испытания, связанные с поиском соотношения «0» и «1» в исследуемой СП. Причина наблюдаемого явления – суммарное «набегание» разницы между уровнем встречаемости нулей и единиц в итоговой двоичной строке, что, в т.ч. может объясняться низкими требованиями к уровню значимости предварительного «просеивания» кубит (Alpha = 0.01). В то же время КВУ ibm_brisbane с аналогичным уровнем значимости продемонстрировал лучшие результаты.

В табл. 2 представлены итоги выполненных экспериментов.

В период исследований при уровне значимости 0.01 для каждого КВУ наименьшее и наибольшее соотношение числа устойчивых кубит составило соответственно: ibm_brisbane – 65/81, ibm_kyvi – 59/73, ibm_sherbrooke – 52/62.

Полученные результаты не являются исчерпывающими и не отражают полную детальную информацию о вычислительных возможностях исследуемых квантовых устройств. Тем не менее, на конкретном примере авторы показали, что подход к использованию квантовых компьютеров в качестве ГСЧ может отразить некоторые качественные аспекты вычислительной системы, которые могут быть полезны в качестве предварительного анализа КВУ при оценке потенциала выбранного компьютера, а также в рамках выбора оптимального набора квантовых состояний (с наилучшими характеристиками) для решения поставленных пользователем прикладных задач.

РЕЗУЛЬТАТЫ И ИХ ОБСУЖДЕНИЕ

По результатам выполненной работы подведем следующие итоги, которые могут послужить отправными точками для предстоящих исследований.

1. Исходя из технических характеристик КВУ, оказывающих воздействие на квантовое состояние, а, следовательно, и на результат генерации СП, встает вопрос о способе определения формальной математической постановки задачи о степени зависимости между актуальными калибровочными параметрами квантового процессора по отношению к ожидаемым результатам процесса КГСЧ. Для примера, в табл. 3 для каждого эксперимента из табл. 2 представлены актуальные характеристики квантового состояния лучшего и худшего кубита всего квантового регистра.

[13] Универсальный тест Маурера не учитывается – недостаточный объем данных. [Maurer's universal test is not taken into account due to a lack of adequate information.]

Таблица 3. Характеристики «крайних» кубит облачных КВУ компании IBM

Дата	КВУ/кубит	Соотношение «0»–«1»	T_1, мкс	T_2, мкс	Readout, err	(sx), err
28.10.2024	brisbane/10	10.000–10.000	290.18	276.91	0.018	$1 \cdot 10^{-4}$
	brisbane/86	12.684–7.316	90.85	115.17	0.113	$1.45 \cdot 10^{-2}$
26.11.2024	brisbane/55	9.999–10.001	243.83	120.25	0.01	$2 \cdot 10^{-4}$
	brisbane/24	7.498–12.502	226.79	98.47	0.14	$2 \cdot 10^{-4}$
05.11.2024	kyvi/5	9.998–10.002	347.03	331.96	0.008	$2 \cdot 10^{-4}$
	kyvi/90	13.029–6.971	43.91	22.84	0.114	$3.3 \cdot 10^{-3}$
24.11.2024	kyvi/122	9.999–10.001	211.81	173.1	0.002	$2 \cdot 10^{-4}$
	kyvi/65	15.143–4.857	201.52	126.32	0.092	$2 \cdot 10^{-3}$
06.11.2024	sherbr-ke/23	9.997–10.003	220.73	24.85	0.009	$4 \cdot 10^{-4}$
	sherbr-ke/56	13.404–6.596	173.46	16.9	0.033	$3 \cdot 10^{-4}$
12.11.2024	sherbr-ke/63	9.984–10.016	217.35	133.31	0.035	$2 \cdot 10^{-4}$
	sherbr-ke/9	12.596–7.404	469.69	70.2	0.035	$2 \cdot 10^{-4}$

Некоторые результаты являются неочевидными. Однако авторы высказывают предположение, что часть кубит может выдавать плохие результаты, в т.ч. при активации соседних квантовых состояний, оказывающих побочное воздействие на искомый кубит. Проверка сформулированного допущения, а также составление математической модели зависимости тактико-технических характеристик КВУ с результатами работы схемы КГСЧ являются следующими возможными направлениями исследования.

2. При использовании всего квантового процессора максимальная длина СП может составить $254 \cdot 10^4$ бит, что дает выборку в ~0.3 МБ при разрядности в 127 кубит и max_shots = 20.000 (количество запусков квантовой схемы). В таком случае, учитывая время обработки квантовой схемы, самым быстрым КВУ является ibm_brisbane (7 секунд), что в идеальном случае предлагает скорость ГСЧ ~44 кБ/сек. Очевидно, такая скорость накладывает ограничения на области применения КВУ в качестве КГСЧ. Более того, как показывают эксперименты, около половины кубит окажется непригодным для получения устойчивой СП. Однако при должном масштабировании разрядности квантовых процессоров и нивелировании существующих ошибок и помех оборудования имеющиеся ограничения могут быть преодолены, что откроет новые возможности применения КВУ в задачах обеспечения информационной безопасности.

3. Тесты NIST STS предложены в 2010 г. и в определенном смысле являются несколько устаревшим способом проверки СП. Авторам видится целесообразным проведение дополнительного исследования генерируемых СП иными, более современными методиками, которые смогут установить не только статистическую (не)зависимость данных, но и характер и природу самого ГСЧ, определив, насколько близко он соответствует свойствам истинно физического КГСЧ.

4. Предложенный подход может войти в расширенный состав набора тестов и программ по оценке технических характеристик исследуемого КВУ. С минимальными временными затратами можно получить предварительную информацию о скорости выполнения квантовых схем на выбранном КВУ. Результат КГСЧ предоставляет сведения об оптимальном наборе кубит, которые могут быть в дальнейшем учтены пользователем при проектировании более сложных и требовательных к техническим ресурсам квантовых схем.

5. В настоящее время многочисленными исследователями ведутся работы, направленные на разработку методов по преодолению свойств декогерентности квантовых состояний [20–22]. Предлагаемые

подходы в большинстве случаев сводятся к применению схем коррекции ошибок и к использованию абстрактного объекта – логического кубита, под которым следует понимать множество физических кубит, совокупно отражающих работу единичного квантового состояния. Однако в контексте задачи КГСЧ, ни применение корректирующих кодов, ни переход к логическим кубитам не видится целесообразным, т.к. идея генерации СП на квантовом компьютере обоснована исключительно при работе с кубитами, выступающими в роли независимых физических ГСЧ.

Авторы планируют включить задачу КГСЧ на облачных КВУ в набор тестов по исследованию вычислительного потенциала квантовых компьютеров для профильных специалистов по информационной безопасности. Программный комплекс будет включать в себя 3 типовых теста: КГСЧ, симуляция протокола ККС ВРК, выполнение квантового преобразования Фурье. Разрабатываемый алгоритм тестирования будет быстрым, простым, доступным с точки зрения затрачиваемых ресурсов КВУ, воспроизводимым, масштабируемым и однозначно интерпретируемым.

С актуальной версией программного кода приложения *QISs*, а также с результатами исследований, можно ознакомиться в репозитории проекта на платформе GitHub[14].

ЗАКЛЮЧЕНИЕ

В рамках проведенного исследования авторами разработано приложение, предлагающее возможность проектирования и удаленного выполнения квантовых схем по ГСЧ на облачных КВУ. В целях определения потенциальной (нежелательной) зависимости между квантовыми состояниями, выступающими в качестве самостоятельных КГСЧ, приложение предлагает дополнительный функционал по корреляционному анализу сгенерированных СП.

По результатам работы программы с помощью частотного побитового теста и на основании выбранного пользователем уровня значимости приложение предоставляет сведения о наиболее и наименее стабильных кубитах с точки зрения надежности и качества применения к квантовым состояниям преобразования Уолша – Адамара.

Для формирования сведений о случайности распределения нулей и единиц в сгенерированных последовательностях в программе предусмотрена возможность проверки полученных СП набором статистических тестов NIST STS.

Предложенный в статье подход может оказаться полезным инструментом в руках исследователей при решении следующих задач: выявление оптимального набора кубит квантового процессора, генерация двоичных СП на квантовых компьютерах, определение некоторых технических возможностей исследуемых квантовых устройств.

БЛАГОДАРНОСТИ

Авторы выражают благодарность студенту РТУ МИРЭА К.Е. Комогорову за оперативную помощь в подготовке bash-скрипта, первичную апробацию программных возможностей приложения *QISs* и предоставление собственного репозитория GitHub для размещения разработанной программы в открытом доступе.

ACKNOWLEDGMENTS

The authors thank K.E. Komogorov, a student at RTU MIREA, for his prompt assistance in preparing the bash script, initial testing of the QISs application software capabilities, and providing his own GitHub repository for hosting the developed program in the public domain.

Вклад авторов

Все авторы в равной степени внесли свой вклад в исследовательскую работу.

Authors' contribution

All authors contributed equally to the research work.

[14] GitHub / QISs. https://github.com/cyberravenman/QISs. Дата обращения 15.05.2025. / Accessed May 15, 2025.

СПИСОК ЛИТЕРАТУРЫ

1. Proctor T., Young K., Baczewski A.D., Blume-Kohout R. Benchmarking quantum computers: *arXiv*. 2024. arXiv:2407.08828. https://doi.org/10.48550/arXiv.2407.08828
2. Amico M., Zhang H., Jurcevic P., et al. Defining Standard Strategies for Quantum Benchmarks. *IBM Publications*. 2023. URL: https://research.ibm.com/publications/defining-standard-strategies-for-quantum-benchmarks. Дата обращения 15.05.2025.
3. Acuaviva A., Aguirre D., Pena R., Sanz M. Benchmarking Quantum Computers: Towards a Standard Performance Evaluation Approach: *arXiv*. 2024. arXiv:2407.10941. https://doi.org/10.48550/arXiv.2407.10941
4. Eisert J., Hangleiter D., Walk N., et al. Quantum certification and benchmarking. *Nat. Rev. Phys.* 2020;2:382–390. https://doi.org/10.1038/s42254-020-0186-4
5. Крючков А.А. О необходимости принятия единого стандарта по оценке производительности и сертификации квантовых вычислительных устройств. *Информационно-экономические аспекты стандартизации и технического регулирования. Сборник научных трудов участников I Научно-практической конференции «Стандартизация: траектория науки», посвященной 100-летию деятельности ФГБУ «Институт стандартизации»*. 2024;6(81):43–49.
6. Wack A., Paik H., Javadi-Abhari A., Jurcevic P., Faro I., Gambetta J.M., Johnson B.R. Scale, Quality, and Speed: three key attributes to measure the performance of near-term quantum computers. *arXiv*. 2021. arXiv:2110.14108. https://doi.org/10.48550/arXiv.2110.14108
7. McKay D.C., Hincks I., Pritchett E.J., Carroll M., Govia L.C.G., Merkel S.T. Benchmarking Quantum Processor Performance at Scale. *arXiv*. 2023. arXiv:2311.05933. https://doi.org/10.48550/arXiv.2311.05933
8. Amico M., Zhang H., Jurcevic P., Bishop L.S., Nation P., Wack A., McKay D.C. Defining Standard Strategies for Quantum Benchmarks. *arXiv*. 2023. arXiv:2303.02108 https://doi.org/10.48550/arXiv.2303.02108
9. Shor P.W. Algorithms for quantum computation: discrete logarithms and factoring. In: *Proceedings 35th Annual Symposium on Foundations of Computer Science*. IEEE; 1994. P. 124–134. https://doi.org/10.1109/SFCS.1994.365700
10. Балыгин К.А., Кулик С.П., Молотков С.Н. Реализация квантового генератора случайных чисел: экстракция доказуемо случайных битовых последовательностей из коррелированных марковских цепочек. *Письма в ЖЭТФ*. 2024;119(7):533–544. https://doi.org/10.31857/S1234567824070115
11. Гайдаш А.А., Гончаров Р.К., Козубов А.В., Яковлев П.В. Математическая модель квантового генератора случайных чисел на основе флуктуации вакуума. *Вестник Санкт-Петербургского университета. Прикладная математика. Информатика. Процессы управления*. 2024;20(2):136–153. https://doi.org/10.21638/spbu10.2024.202
12. Петренко А.А., Ковалев А.В., Бугров В.Е. Генерация случайных чисел с использованием массива связанных лазеров на основе микростолбиков с квантовыми точками. *Научно-технический вестник информационных технологий, механики и оптики.* 2021;21(6):962–968. https://doi.org/10.17586/2226-1494-2021-21-6-962-968
13. Орлов М.А., Нечаев К.А., Резниченко С.А. Оценка статистических свойств и криптографической стойкости случайных последовательностей, полученных квантовым компьютером IBM. *Безопасность информационных технологий*. 2023;30(1):14–26. http://doi.org/10.26583/bit.2023.1.01
14. Li Y., Fei Y., Wang W., et al. Quantum random number generator using a cloud superconducting quantum computer based on source-independent protocol. *Sci Rep.* 2021;11:23873. https://doi.org/10.1038/s41598-021-03286-9
15. Salehi R., Razaghi M., Fotouhi B. Hybrid Hadamard and Controlled-Hadamard Based Quantum Random Number Generators in IBM QX. *Physica Scripta*. 2022;97(6):065101. https://doi.org/10.1088/1402-4896/ac698b
16. Yadav A., Mishra S., Pathak A. Partial loopholes free device-independent quantum random number generator using IBM's quantum computers. *Physica Scripta*. 2024;99(11):115103. https://doi.org/10.1088/1402-4896/ad7c02
17. Feynman R.P. Quantum Mechanical Computers. *Optics News*. 1985;11(2):11–20. URL: https://www.optica-opn.org/home/articles/on/volume_11/issue_2/features/quantum_mechanical_computers/. Дата обращения 15.05.2025. /. Accessed May 15, 2025.
18. Крючков А.А. *QISs_v.0.3.9*: свидетельство о государственной регистрации Программы для ЭВМ RU 2025613655 РФ. Заявка № 2025611456; заявл. 28.01.2025; опубл. 13.02.2025. Бюл. № 2.
19. Крючков А.А., Комогоров К.Е. Моделирование процесса генерации случайных чисел на квантовых вычислительных устройствах. В сб.: *Материалы VIII НПК «Актуальные проблемы и перспективы радиотехнических и инфокоммуникационных систем»* (18–22 ноября 2024 г., Москва). М.: РТУ МИРЭА; 2024. С. 501–506.
20. Acharya R., Abanin D.A., Aghababaie-Beni L., et al. Quantum error correction below the surface code threshold. *Nature*. 2025;638:920–926. https://doi.org/10.1038/s41586-024-08449-y
21. Verma S., Kumari S.S., Kumar R.S. Topological quantum error correction with semions. *Int. J. Phys. Math*. 2024:6(2):44–47. https://doi.org/10.33545/26648636.2024.v6.i2a.95
22. Webster M., Browne D. Engineering Quantum Error Correction Codes Using Evolutionary Algorithms. *IEEE Trans. Quantum Eng*. 2025;6:3100514. https://doi.org/10.1109/TQE.2025.3538934

REFERENCES

1. Proctor T., Young K., Baczewski A.D., Blume-Kohout R. Benchmarking quantum computers. *arXiv*. 2024. arXiv:2407.08828. https://doi.org/10.48550/arXiv.2407.08828
2. Amico M., Zhang H., Jurcevic P., et al. Defining Standard Strategies for Quantum Benchmarks. *IBM Publications*. 2023. Available from URL: https://research.ibm.com/publications/defining-standard-strategies-for-quantum-benchmarks. Accessed May 15, 2025.

3. Acuaviva A., Aguirre D., Pena R., Sanz M. Benchmarking Quantum Computers: Towards a Standard Performance Evaluation Approach. *arXiv*. 2024. arXiv:2407.10941. https://doi.org/10.48550/arXiv.2407.10941
4. Eisert J., Hangleiter D., Walk N., et al. Quantum certification and benchmarking. *Nat. Rev. Phys.* 2020;2:382–390. https://doi.org/10.1038/s42254-020-0186-4
5. Kryuchkov A.A. On the need to adopt a single standard for evaluating the performance and certification of quantum computers. *Informatsionno-ehkonomicheskie aspekty standartizatsii i tekhnicheskogo regulirovaniya = Information and Economic Aspects of Standardization and Technical Regulation.* 2024;6(81):43–49 (in Russ.).
6. Wack A., Paik H., Javadi-Abhari A., Jurcevic P., Faro I., Gambetta J.M., Johnson B.R. Scale, Quality, and Speed: three key attributes to measure the performance of near-term quantum computers. *arXiv*. 2021. arXiv:2110.14108. https://doi.org/10.48550/arXiv.2110.14108
7. McKay D.C., Hincks I., Pritchett E.J., Carroll M., Govia L.C.G., Merkel S.T. Benchmarking Quantum Processor Performance at Scale. *arXiv*. 2023. arXiv:2311.05933. https://doi.org/10.48550/arXiv.2311.05933
8. Amico M., Zhang H., Jurcevic P., Bishop L.S., Nation P., Wack A., McKay D.C. Defining Standard Strategies for Quantum Benchmarks. *arXiv*. 2023. arXiv:2303.02108 https://doi.org/10.48550/arXiv.2303.02108
9. Shor P.W. Algorithms for quantum computation: discrete logarithms and factoring. In: *Proceedings 35th Annual Symposium on Foundations of Computer Science*. IEEE; 1994. P. 124–134. https://doi.org/10.1109/SFCS.1994.365700
10. Balygin K.A., Kulik S.P., Molotkov S.N. Implementation of a Quantum Generator of Random Numbers: Extraction of Provably Random Bit Sequences from Correlated Markov Chains. *Jetp. Lett.* 2024;119(7):538–548. https://doi.org/10.1134/S0021364024600575
[Original Russian Text: Balygin K.A., Kulik S.P., Molotkov S.N. Implementation of a Quantum Generator of Random Numbers: Extraction of Provably Random Bit Sequences from Correlated Markov Chains. *Pis'ma v Zhurnal ehksperimental'noi i teoreticheskoi fiziki* (*Pis'ma v ZHEHTF*). 2024;119(7):533–544 (in Russ.). https://doi.org/10.31857/S1234567824070115]
11. Gaidash A.A., Goncharov R.K., Kozubov A.V., Yakovlev P.V. Mathematical model of random number generator based on vacuum fluctuations. *Vestnik Sankt-Peterburgskogo universiteta. Prikladnaya matematika. Informatika. Protsessy upravleniya = Vestnik of Saint Petersburg University. Applied Mathematics. Computer Science. Control Processes.* 2024;20(2):136–153 (in Russ.). https://doi.org/10.21638/spbu10.2024.202
12. Petrenko A.A., Kovalev A.V., Bougrov V.E. Random number generation with arrays of coupled quantum-dot micropillar lasers. *Nauchno-tekhnicheskii vestnik informatsionnykh tekhnologii, mekhaniki i optiki = Scientific and Technical Journal of Information Technologies, Mechanics and Optics*. 2021;21(6):962–968 (in Russ.). https://doi.org/10.17586/2226-1494-2021-21-6-962-968
13. Orlov M.A., Nechaev K.A., Reznichenko S.A. Evaluation of statistical properties and cryptographic strength of random sequences obtained by an IBM quantum computer. *Bezopasnost' informatsionnykh tekhnologii = IT Security* (Russia). 2023;30(1):14–26 (in Russ.). http://doi.org/10.26583/bit.2023.1.01
14. Li Y., Fei Y., Wang W., et al. Quantum random number generator using a cloud superconducting quantum computer based on source-independent protocol. *Sci Rep.* 2021;11:23873. https://doi.org/10.1038/s41598-021-03286-9
15. Salehi R., Razaghi M., Fotouhi B. Hybrid Hadamard and Controlled-Hadamard Based Quantum Random Number Generators in IBM QX. *Physica Scripta*. 2022;97(6):065101. https://doi.org/10.1088/1402-4896/ac698b
16. Yadav A., Mishra S., Pathak A. Partial loopholes free device-independent quantum random number generator using IBM's quantum computers. *Physica Scripta*. 2024;99(11):115103. https://doi.org/10.1088/1402-4896/ad7c02
17. Feynman R.P. Quantum Mechanical Computers. *Optics News*. 1985;11(2):11–20. Available from URL: https://www.optica-opn.org/home/articles/on/volume_11/issue_2/features/quantum_mechanical_computers/. Accessed May 15, 2025.
18. Kryuchkov A.A. *QISs_v.0.3.9*: Computer Program RU2025613655 RF. Publ. 13.02.2025 (in Russ.).
19. Kryuchkov A.A., Komogorov K.E. Simulation of the random number generation process on quantum computing devices. In: *Proceedings of the 8th Scientific and Practical Conference "Actual Problems and Prospects of Radio Engineering and Infocommunication Systems."* Moscow: RTU MIREA; 2024. P. 501–506 (in Russ.).
20. Acharya R., Abanin D.A., Aghababaie-Beni L., et al. Quantum error correction below the surface code threshold. *Nature*. 2025;638:920–926. https://doi.org/10.1038/s41586-024-08449-y
21. Verma S., Kumari S.S., Kumar R.S. Topological quantum error correction with semions. *Int. J. Phys. Math*. 2024:6(2):44–47. https://doi.org/10.33545/26648636.2024.v6.i2a.95
22. Webster M., Browne D. Engineering Quantum Error Correction Codes Using Evolutionary Algorithms. *IEEE Trans. Quantum Eng*. 2025;6:3100514. https://doi.org/10.1109/TQE.2025.3538934

Об авторах

Корольков Андрей Вячеславович, к.т.н., член-корреспондент Академии криптографии Российской Федерации, член-корреспондент Академии Инженерных наук им. А.М. Прохорова Российской Федерации, заведующий кафедрой информационной безопасности, Институт искусственного интеллекта, ФГБОУ ВО «МИРЭА – Российский технологический университет», (119454, Россия, Москва, пр-т Вернадского, д. 78). E-mail: korolkov@mirea.ru. SPIN-код РИНЦ 3849-6868, https://orcid.org/0009-0003-4862-4816

Крючков Андрей Андреевич, старший преподаватель, кафедра информационной безопасности, Институт искусственного интеллекта, ФГБОУ ВО «МИРЭА – Российский технологический университет» (119454, Россия, Москва, пр-т Вернадского, д. 78). E-mail: kryuchkov_a@mirea.ru. SPIN-код РИНЦ 7117-7238, https://orcid.org/0009-0002-4750-6204

About the Authors

Andrey V. Korolkov, Cand. Sci. (Eng.), Corresponding Member of the Academy of Cryptography of the Russian Federation, Corresponding Member of the A.M. Prokhorov Academy of Engineering Sciences of the Russian Federation, Head of the Department of Information Security, Institute of Artificial Intelligence, MIREA – Russian Technological University (78, Vernadskogo pr., Moscow, 119454 Russia). E-mail: korolkov@mirea.ru. RSCI SPIN-code 3849-6868, https://orcid.org/0009-0003-4862-4816

Andrey A. Kryuchkov, Senior Lecturer, Department of Information Security, Institute of Artificial Intelligence, MIREA – Russian Technological University (78, Vernadskogo pr., Moscow, 119454 Russia). E-mail: kryuchkov_a@mirea.ru. RSCI SPIN-code 7117-7238, https://orcid.org/0009-0002-4750-6204